КІБЕРБЕЗПЕКА НА МОРСЬКОМУ ТРАНСПОРТІ ЯК ПРІОРИТЕТНА ЗАДАЧА ПІДГОТОВКИ СПЕЦІАЛІСТІВ МОРСЬКОГО ПРОФІЛЮ

Камінська Наталія Геннадіївна
ORCID ID: 0000-0002-9975-7403
викладач кафедри інноваційних технологій та технічних засобів судноводіння
Херсонська державна морська академія, Україна

В останній час світова економіка повною мірою відчула на собі вплив кіберзлочинності на всі процеси, які відбуваються фактично в будь якій сфері діяльності. Проблема кіберзахисту потребувала термінового вирішення на самому високому рівні. Великі компанії на підставі детального аналізу зробили висновки про те що потрібно мати глобальний захист від кібератак, як технологічний, так й ресурсний, тобто наявність професіоналів які зможуть контролювати ситуацію з кібернебезпекою та вчасно приймати вірні управлінські рішення.

Не уникла цієї проблеми і така галузь як морський транспорт, якій є основою інфраструктури глобальних ланцюгів поставок. Поява нових судноплавних компаній, постійний зріст вантажомісткості морських суден, їх кількості сприяє стабільності світових товарних ринків та скороченню транспортних витрат, та в той же час підвищує конкуренцію між компаніями, до того ж викликає велику зацікавленість шахраїв, які бажають скористатися ситуацією що склалася.

Основним законом, який регулює дії із забезпечення кібербезпеки у всіх сферах діяльності в Україні, є Закон України «Про основні засади забезпечення кібербезпеки України» [1]. Цей Закон визначає правові та організаційні основи забезпечення захисту життєво важливих інтересів людини і громадянина, суспільства та держави, національних інтересів України у кіберпросторі, основні цілі, напрями та принципи державної політики у сфері кібербезпеки, повноваження державних органів, підприємств, установ, організацій, осіб та громадян у цій сфері, основні засади координації їхньої діяльності із забезпечення кібербезпеки.

Питання кібербезпеки є максимально актуальними в галузі морських перевезень. Це пов'язано з багатьма факторами. Відомо, що більш ніж 80% всього об'єму світової товарної торгівлі здійснюється саме морським транспортом, та з кожним роком цій показник тільки збільшується. Це означає велику конкуренцію серед перевізників за вигідні фрахти, та, відповідно, велику цінність інформації про все що відбувається у цієї сфері. Оскільки вартість вантажу що доставляють морськими шляхами дуже велика, приватна інформація компаній щодо перевезень є ціллю різного роду кіберзлочинців, хакерів, навіть піратів, які досі представляють небезпеку для морських суден, особливо у південних акваторіях. До речи, пірати дуже ефективно користуються інформацією про трафік суден, склад екіпажу, вартість вантажу, всі ці відомості вони отримують від кіберзлочинців за великі кошти, та використовують їх для нападу на морські судна. Тому захист інформації є «питанням номер один» для будь якого морського судна.

Автоматизація всіх процесів на суднах, портах та терміналах значно підвищує ефективність їх роботи, підвищує надійність функціонування всього комплексу обслуговування морських перевезень та швидкість обробки інформації та прийняття управлінських рішень. Але поруч з підвищенням якості роботи всіх складових цього процесу підвищується також і небезпека кібератак на інфраструктуру морської галузі. Наслідки таких явищ можуть бути непередбачені.

Отже, як ми можемо оцінити ситуацію яка склалася. Розглянемо лише один напрямок цієї проблеми, а саме, наявність інформації щодо місця знаходження судна, тобто його координати, широту та довготу.

З одного боку, відповідно до вимог Конвенції Міжнародної морської організації з охорони життя на морі [2], судно зобов'язано надавати інформацію щодо свого місцяположення, з метою регулювання переміщень суден що перебувають на достатньої близькості у морському просторі, контролю з боку власників суден та портових служб. Як правило, більшість суден користуються для цього автоматичними ідентифікаційними системами для передачі інформації, яка стосується безпосередньо самого судна. Але, з іншого боку, вся ця інформація передається на відкритих частотах, що є небезпечним з точки зору перехоплення її небажаними суб'єктами (наприклад, хакерами або кіберзлочинцями) та подальшого використання у кібератаках, які можуть привести до фатальних наслідків. Якщо з метою захисту від кібератак або розсекречування даних, особливо в небезпечних зонах, екіпаж судна тимчасово відключає автоматизовані інформаційні системи, це може привести до того що під час лиха берегові служби не зможуть допомогти, оскільки не будуть мати інформацію про місцезнаходження цього судна. Тому потрібно обрати таку стратегію захисту, яка максимально забезпечить судну як захист від кібератак, так і гарантовану підтримку з боку берегових служб.

Обрана стратегія базується в першу чергу на якісній підготовці фахівців морського профілю, яка враховує не тільки безпосередньо надання знань з судноводіння, суднового обладнання та всього що пов'язано з роботою в цієї галузі, а й навичок безпечного користування сучасними засобами зв'язку, захисту інформації, вміння протистояти кібератакам. Херсонська державна морська академія цілком відповідає вимогам підготовки фахівців морської галузі з урахуванням вирішення проблем кібербезпеки судна. Розроблена програма курсу «Кібербезпека та цифрові технології» охоплює всі можливі питання які можуть виникнути у судноводія під час виконання ним своїх обов'язків на борту судна [3]. Отже, одним з найважливіших питань є вивчення методів зменшення загроз втрати або розповсюдження даних додатковим шифруванням ідентифікаційних та всіх інших відомостей, введення систем двофакторної автентифікації, використання хмарних технологій збереження та передачі даних. На опрацювання цих тем виділено багато часу та розроблено відповідне методичне забезпечення, що дозволяє не тільки засвоїти теоретичний матеріал, а й отримати практичні навички протидії кіберзлочинам на морському судні. Тут потрібно вказати, що для досягнення кращих результатів, які б забезпечили конкурентоспроможність випускників академії на світовому ринку праці, викладачами цієї дисципліни розроблені власні методики. Надійний захист даних передбачає знання багатьох сучасних способів та вміння знаходити найнадійніший у кожній конкретній ситуації. В цьому і полягає професійний підхід до навчання майбутніх навігаторів та, відповідно, отримання гідних спеціалістів морської галузі.

Список використаних джерел:

1. Закон України «Про основні засади забезпечення кібербезпеки України» (Відомості Верховної Ради (ВВР), 2017, № 45, ст.403) https://zakon.rada.gov.ua/laws/show/2163-19#Text
2. Міжнародна конвенція про підготовку і дипломування моряків та несення вахти. (2011). Лондон.: IMO. «Эшфорд Пресс» https://ips.ligazakon.net/document/view/mu78k01u?ed=2010_06_25
3. Voloshynov,S., Kravtsova,L. & Zaytseva,T. (2021). Development of a methodology for a systematic approach to cyber security problems on board a ship. Maritime security of the Baltic-Black Sea region: challenges and threats. Riga: Izdevnieciba «Baltija Publishing». С.19–23.